

<u>SYMBOL</u>	<u>DESCRIPTION</u>
$f()$	ALICE'S AND BOB'S COMBINING FUNCTION
I_A, I_B	ALICE'S AND BOB'S DISCARDABLE INITIALIZATION VECTOR
K_A, K_B	ALICE'S AND BOB'S PRIVATE SESSION KEY
M_A, M_B	ALICE'S AND BOB'S PUBLIC KEY
N_A, N_B	ALICE'S AND BOB'S RANDOM NONCE FOR KEY VERIFICATION
N_A+1, N_B+1	MODIFIED (INCREMENTED) RANDOM NONCES
α, β	ALICE'S AND BOB'S CONGRUENT EXPONENTIAL BASE; (ALICE'S AND BOB'S MODULO VARIABLE)
P_A, P_B	ALICE'S AND BOB'S SECRET PASSWORDS
R_A, R_B	ALICE'S AND BOB'S PRIVATE RANDOM NUMBERS
S_A, S_B	ALICE'S AND BOB'S HIGH-ENTROPY SECRET
$(Y)_x$	ENCRYPT CLEARTYPE, Y, WITH KEY X
$(Z)^{-1}_x$	DECRYPT CIPHERTEXT, Z, WITH KEY X
$(N_s)_{x_{n-2}}$	SUPERENCRYPT PLAINTEXT, N_s , WITH VARIABLE KEYS n

FIG. 1

Alice 202	XMSN	Bob 204
Generate R_A 206		Generate R_B 208
$M_A = \alpha^{R_A} \text{ mod } \beta$ 210		$M_B = \alpha^{R_B} \text{ mod } \beta$ 212
transmit M_A 214	214	$K_B = (M_A)^{R_B} \text{ mod } \beta$ 216
$K_A = (M_B)^{R_A} \text{ mod } \beta$ 220	218	transmit M_B 218
CONTINUE 222		CONTINUE 226
Encrypted 224 Two way transmissions	230 ↔	Encrypted 228 Two way transmissions

FIG. 2

(Prior Art)

Alice 202	XMSN	Bob 204
Generate N_A 302		Generate N_B 304
encrypt N_A as $(N_A)_{K_A}$ 306		
transmit $(N_A)_{K_A}$ 308	308	$N_A = ((N_A)_{K_A})^{-1}_{K_B}$ 310
		increment N_A as N_A+1 312
		encrypt $(N_B, N_A+1)_{K_B}$ 314
N_B 320, N_A+1 322 = $((N_B, N_A+1)_{K_B})^{-1}_{K_A}$ 318	316	transmit $(N_B, N_A+1)_{K_B}$ 316
increment N_B as N_B+1 324		
encrypt $(N_B+1)_{K_A}$ 326		
transmit $(N_B+1)_{K_A}$ 328	328	$N_B+1 = ((N_B+1)_{K_A})^{-1}_{K_B}$ 330
verify N_A+1 332		verify N_B+1 340
If true, Bob 204 and Alice 202 share the same session key ($K_A = K_A$) CONTINUE 336	334 If false STOP	342 If true, Alice 204 and Bob 204 share the same session key ($K_A = K_A$) CONTINUE 344
Encrypted 338 Two way transmissions	348 ↔	Encrypted 346 Two way transmissions

FIG. 3

(Prior Art)

Alice 402		XMSN	Bob 404	
store password P_A 406 and identity 408 410			store password P_B 414 and identity 416 412	
Generate N_A 418			Generate N_B 420	
transmit identity 408, and service request 424 422		422 ---->	obtain password P_B 414 and identity 416 from identity 408 424	
			verify identity 408 = identity 416 426	
			If true, 430 Alice 403 is IDENTIFIED to Bob 404, CONTINUE	
encrypt N_B as $(N_B)_{P_A}$ 440		438	transmit N_B 438	
transmit N_A 418, $(N_B)_{P_A}$ 440 442		442 ---->	verify $N_B = ((N_B)_{P_A})^{-1}_{P_B}$ 444	
			If true, 448 Alice 402 is AUTHENTICATED to Bob 404, CONTINUE	
			If false STOP	
			encrypt N_A as $(N_A)_{P_B}$ 450	
verify $N_A = ((N_A)_{P_B})^{-1}_{P_A}$ 454		452	transmit $(N_A)_{P_B}$ 452	
If true, Bob 404 is AUTHENTICATED to Alice 402, CONTINUE 458		456 If false STOP	CONTINUE 462	
Unencrypted Two way transmissions 460		466	Unencrypted Two way transmissions 464	

FIG. 4

Alice 502	XMSN	Bob 504					
store password P_A 506 and identity 508 510		store password P_B 514 and identity 516 512					
Generate R_A 518		Generate R_B 522 and N_B 524					
$M_A = (\alpha)^{R_A} \text{ mod } B$ 526		$M_B = (\alpha)^{R_B} \text{ mod } B$ 528					
transmit identity 508, M_A 526, and service request 532 530	530 ---->	obtain password P_B 514 and identity 516 based on identity 508 534					
		verify identity 508 = identity 516 536					
		<table><tr><td rowspan="2">If true, Alice 502 is IDENTIFIED to Bob 504; CONTINUE</td><td colspan="2">If false 538</td></tr><tr><td>generate random P_B 542; CONTINUE</td><td>STOP 540</td></tr></table>	If true, Alice 502 is IDENTIFIED to Bob 504; CONTINUE	If false 538		generate random P_B 542; CONTINUE	STOP 540
If true, Alice 502 is IDENTIFIED to Bob 504; CONTINUE	If false 538						
	generate random P_B 542; CONTINUE	STOP 540					
		$K = K_B = (M_A)^{R_B} \text{ mod } B$ 546					
		$S = S_B = f(P_B, M_A, M_B)$ 548					
		encrypt N_B as $(N_B)_S$ 550					
		encrypt $(N_B)_S$ as $((N_B)_S)_K$					
$K = K_A = (M_B)^{R_A} \text{ mod } B$ 556	558	transmit $M_B, ((N_B)_S)_K$ 554					
$S = S_A = f(P_A, M_A, M_B)$ 558							
$N_B = (((N_B)_S)_K)^{-1} \cdot S$ 560							
Generate N_A 562							
modify N_B as $N_B + 1$ 564							
encrypt $N_A, N_B + 1$ as $(N_A, N_B + 1)_S$ 566							
encrypt $(N_A, N_B + 1)_S$ as $((N_A, N_B + 1)_S)_K$ 568							
transmit $((N_A, N_B + 1)_S)_K$ 570	570	N_A 574, $N_B + 1$ 576 = $((N_A, N_B + 1)_S)_K^{-1} \cdot S$ 572					
		verify $N_B + 1$ 576 - 1 = N_B 524 578					
		<table><tr><td rowspan="2">If true, Alice 502 is AUTHENTICATED to Bob 504; CONTINUE</td><td rowspan="2">580</td><td>If false STOP</td></tr><tr><td></td></tr></table>	If true, Alice 502 is AUTHENTICATED to Bob 504; CONTINUE	580	If false STOP		
If true, Alice 502 is AUTHENTICATED to Bob 504; CONTINUE	580	If false STOP					
One way transmissions	582 -->	<table><tr><td>Open one way link</td><td>generate I_B</td></tr></table>	Open one way link	generate I_B			
Open one way link	generate I_B						

FIG. 5A

Alice 502		XMSN	Bob 504	
			If true, 580 Alice 502 is AUTHENTICATED to Bob 504; CONTINUE	If 579 false STOP
One way transmissions 582	582 →		Open one way link 581	generate 583 I_B
			modify N_A as N_A+1 584	
			encrypt I_B, N_A+1 as 586 $(I_B, N_A+1)_S$	
			encrypt $(I_B, N_A+1)_S$ as 588 $((I_B, N_A+1)_S)_K$	
I_B 591, N_A+1 592 = 590 $((((I_B, N_A+1)_S)_K)^{-1}_K)^{-1}_S$		589 ←	transmit $((I_B, N_A+1)_S)_K$ 589	
verify 593 N_A+1 592 - 1 = N_A 562			CONTINUE 597	
If true, Bob 504 is IDENTIFIED and AUTHENTICATED to Alice 502, CONTINUE 595	594 If false STOP			
Encrypted 596 Two way transmissions		599 ↔	Encrypted 598 Two way transmissions	

FIG. 5B

Alice 602	XMSN	Bob 604
store password P_A 606 and identity 608 610		store password P_B 614 and identity 616
Generate R_A 620 and N_A 622		Generate R_B 626 and N_B 628 624
$M_A = (\alpha)^{R_A} \bmod \beta$ 630		$M_B = (\alpha)^{R_B} \bmod \beta$ 632
encrypt N_A as $(N_A)_E$ 634		
transmit identity 608, M_A 630, $(N_A)_E$ 634, and service request 638 636	636	obtain password P_B 614 and identity 616 based on identity 608 640
		verify identity 608 = identity 616 642
		<div> <div>If true, Alice 602 is IDENTIFIED to Bob 604; CONTINUE</div> <div> <div>If false, 644</div> <div> <div>generate random P_B 648; CONTINUE</div> <div>646 STOP</div> </div> </div> </div>
		$N_A = ((N_A)_E)^{-1}_{R_B}$ 652
		$K = K_B = (M_A)^{R_B} \bmod \beta$ 654
		$S = S_B = f(P_B, M_A, M_B)$ 656
		modify N_A as N_A+1 658
		encrypt (N_B, N_A+1) as $((N_B, N_A+1)_E)$ 660
		encrypt $(N_B, N_A+1)_E$ as $((N_B, N_A+1)_E)_E$ 662
$K = K_A = (M_B)^{R_A} \bmod \beta$ 665	665	transmit $M_B, ((N_B, N_A+1)_E)_E$ 664
$S = S_A = f(P_A, M_A, M_B)$ 668		
N_B 672, N_A+1 674 = $((((N_B, N_A+1)_E)_E)^{-1}_{R_A})^{-1}_{R_A}$ 670		
verify N_A+1 674 - 1 = N_A 622 676		
<div>If true, Bob 604 is IDENTIFIED and AUTHENTICATED to Alice 502; CONTINUE 678</div> <div>If false STOP</div>	677	
Open one way link 679	680	One way transmissions 680
generate I_A 681		

FIG. 6A

603

Alice 602		XMSN	Bob 604	
If true, Bob 604 is IDENTIFIED and AUTHENTICATED to Alice 502; 678 CONTINUE 678		677 If false STOP		
Open one way link 679		680	One way transmissions 680	
generate I_A 681				
modify N_B as N_B+1 682				
encrypt I_A, N_B+1 as $(I_A, N_B+1)_S$ 683				
encrypt $(I_A, N_B+1)_S$ as $((I_A, N_B+1)_S)_K$ 684				
transmit $((I_A, N_B+1)_S)_K$ 685		685	$I_{A_B} 687, N_B+1 688 = (((I_A, N_B+1)_S)_K)^{-1}_K)^{-1}_S$ 686	
CONTINUE 696			verify $N_B+1 688 - 1 = N_B 628$ 690	
			If true, Alice 602 is AUTHENTICATED to Bob 604; CONTINUE 693 If false STOP 692	
Encrypted 698 Two way transmissions		699	Encrypted 694 Two way transmissions	

FIG. 6B

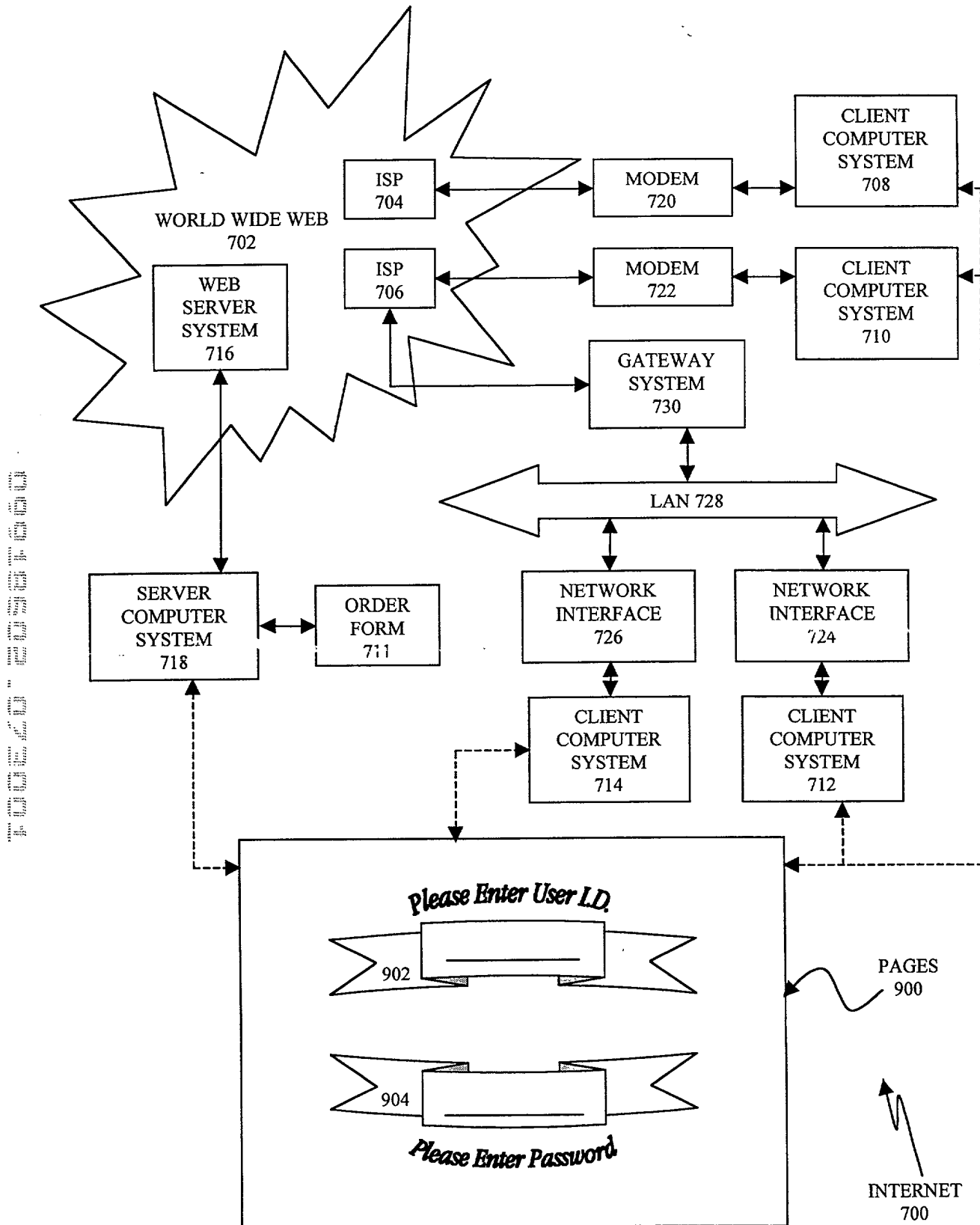


FIG. 7

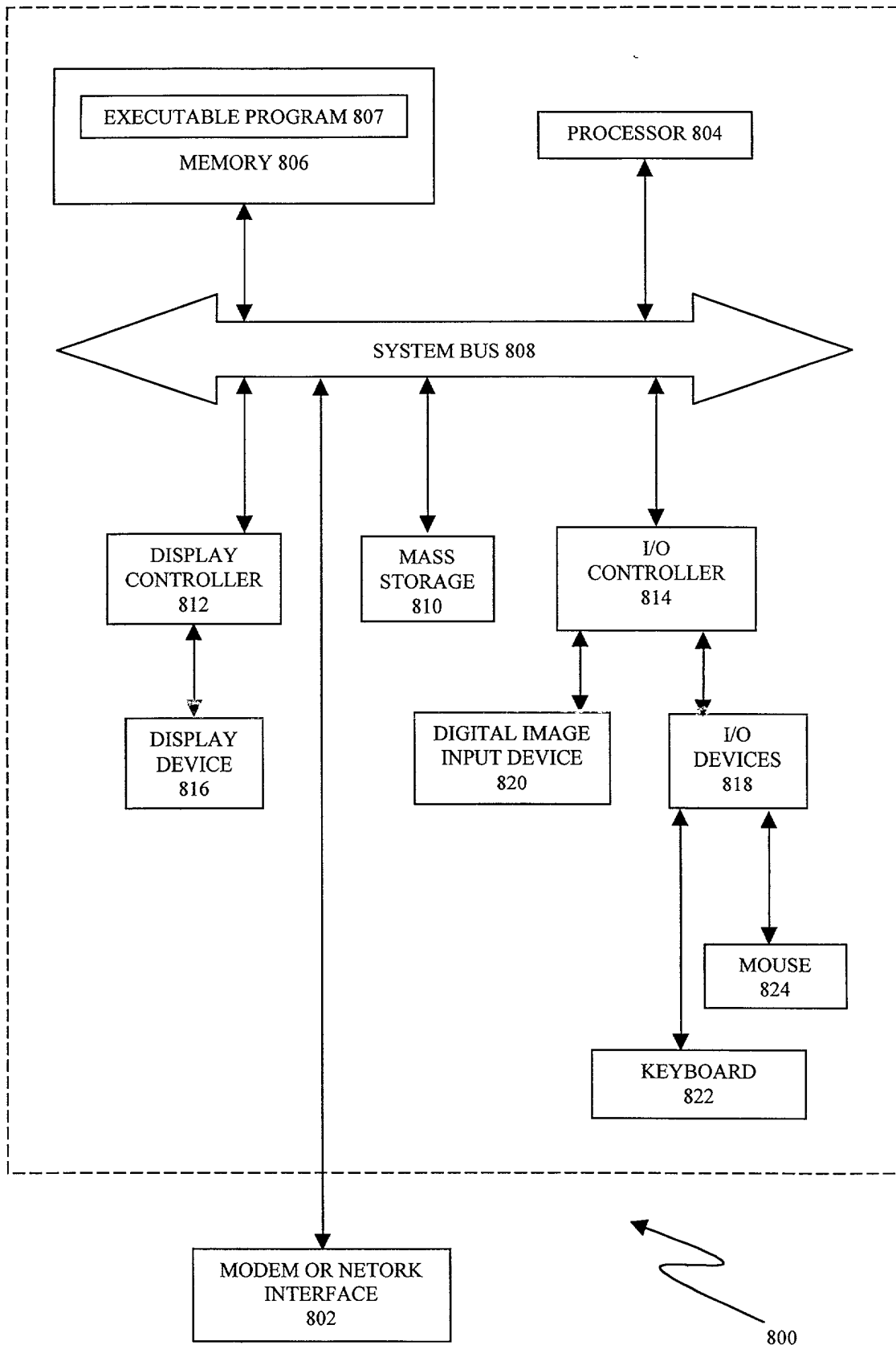


FIG. 8